UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/594,368	06/15/2000	Herb A. Little	555255012130	8507

7590 07/15/2004

David B Cochran
Jones Day Reavis & Pogue
North Point
901 Lakeside Avenue
Cleveland, OH 44114

EXAMINER	
NORRIS, TREMAYNE M	

ART UNIT	PAPER NUMBER
2137	6

DATE MAILED: 07/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/594,368	LITTLE, HERB A.	
	Examiner	Art Unit	
	Tremayne M. Norris	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 April 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-45* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 April 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed on 4/16/04 have been fully considered but they are not persuasive.

Applicant argues that the Vanstone reference does not teach that the encryption step of producing an ephemeral key pair is done before the signing operation and questions that the key pair produced in the Vanstone reference is even ephemeral. Examiner feels that this element is found in the Vanstone reference. In col.3 lines 3-12, Vanstone teaches of an ephemeral private key (x) and an ephemeral public key ($f(\alpha)^{g(x)}$) are generated (col.3 lines 3-6). From that key pair a signature (s_A) is produced (col.3 lines 7-9), therefore the encryption step indeed comes before the signing operation. This key pair is ephemeral because they are produced each time a session key is required (col.2 lines 18-19), thus they only last for a short period of time.

Applicant also agues that the step of generating the digital signature includes hashing the plaintext message is not found in the Vanstone reference either. However, through the applicant's own admission of prior art, this feature is already known in the art (page.8 lines 5-17).

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1,2,4-8, 16-23, 31-40 are rejected under 35 U.S.C. 102(e) as being anticipated by Vanstone et al.

Regarding Claims 1 ,16, 31, Vanstone et al teach:

A public-key encryption process and system comprising the steps of:

a) encrypting a plaintext message into a ciphertext message, the encrypting step includes the step of producing an ephemeral key pair ;

b) signing a digital signature using the ephemeral key pair (col.3 lines 3-12).

Regarding Claims 2,17, 32 Vanstone et al teach a public-key encryption process wherein the encrypting step uses an El Gamal encryption scheme (col.4 lines 3-51).

Regarding Claims 4,19,34, Vanstone et al teach:

A public-key encryption process and system, wherein the step of producing the ephemeral key pair comprises the steps of generating an encryption ephemeral private

key x and calculating an encryption ephemeral public key X = xG, where G is a generator (col.3 lines 3-6).

Regarding Claims 5,20,35, Vanstone et al teach:

A public-key encryption process and system, for encrypting messages for communication between a sender and a receiver, the process further comprising the steps of,

at the sender,

a) generating a sender private key a; and

b) calculating a sender public key A = aG, where G is a generator,

and at the receiver,

a) generating a receiver private key b; and

b) calculating a receiver public key *B = bG,*

wherein the sender obtains an authentic copy of the receiver public key *B* and the receiver obtains an authentic copy of the sender public key A (col.4 lines 3-14).

Regarding Claims 6,21,36, Vanstone et al teach:

A public-key encryption process and system, wherein the step of producing the ephemeral key pair comprises the steps of generating an encryption ephemeral private key x and calculating an encryption ephemeral public key X = xG (col.3 lines 7-9).

Regarding Claims 7,22,27, Vanstone et al teach:

A public-key encryption process and system, further comprising the steps of, at the sender, generating a secret key $K = xB$ and encrypting a plaintext message using the secret key K to generate a ciphertext message (col.3 lines 28-31 and lines 49-53).

Regarding Claims 8, 23,38 Vanstone et al teach:

A public-key encryption process and system, further comprising the steps of, at the sender, using the encryption private key x as a signature ephemeral private key and using the encryption ephemeral public key X as a signature ephemeral public key to generate a digital signature (col.3 lines 7-9).

Regarding Claims 9,24,29, Vanstone et al teach:

A public-key encryption process and system, wherein the digital signature comprises a first value r and a second value s, the process further comprising the step of, at the sender, transmitting the encryption ephemeral public key X, the ciphertext message and the second value s of the digital signature to the receiver (col.3 lines 10-12 and col.4 lines 38-39).

Regarding Claims 10,25,40 Vanstone et al teach;

A public-key encryption process and system, further comprising the steps of, at the receiver, generating the secret key $K = bX$, decrypting the transmitted ciphertext message using the generated secret key K, calculating the first value r of the digital

signature using the decrypted message and the transmitted encryption ephemeral public key X and validating the digital signature based on the calculated first value r and the transmitted second value s (col.3 lines 22-31 and lines 57-58).

Regarding claims 18 and 33, Vanstone teaches a public-key encryption process wherein the step of signing a digital signature comprises generating the digital signature using a Nyberg-Rueppel digital signature scheme (col.4 lines 3-51);

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone, and further in view of applicant's own prior art admission.

Regarding claim 3, Vanstone teaches a public-key encryption process wherein the step of signing a digital signature comprises generating the digital signature using a Nyberg-Rueppel digital signature scheme (col.4 lines 3-51), but does not teach the step

of generating the digital signature includes hashing the plaintext. Applicant teaches the step of generating the digital signature includes hashing the plaintext through applicant's own prior art admission (page.8 lines 5-17). It would have been obvious to one of ordinary skill in the art to combine Vanstone's key agreement transport protocol with the teachings of hashing plaintext to generate digital signature in order to save time and space by signing the hash of plaintext as oppose to signing the plaintext directly which would typically involve splitting the plaintext into blocks and signing each block. Hashing also allows for efficient data integrity checks.

6. Claims 11-15, 26-30, 41-45 rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone et al as applied to claim1 above, and further in view of Heer.

Regarding claims 11-15, 26-30, and 41-45, Vanstone et al teach an encryption process of encrypting plaintext message into ciphertext message using an ephemeral key pair and signing a digital signature using the ephemeral key pair. Vanstone et al do not teach an encryption process implemented in a wireless communication system or device, but Heer et al do. It would be obvious to one of ordinary skill in the art to employ a public key encryption process with use of wireless communication systems

and devices in order to protect information being sent and received from being corrupted and tampered with (col.1 lines 28-38).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tremayne M. Norris whose telephone number is (703) 305-8045. The examiner can normally be reached on M-F 7:30AM-5:00PM alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703) 305-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Tremayne Norris

June 30, 2004

MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137